

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷

H04Q 7/32

H04L 29/06

//H04Q7/38



[12] 发明专利说明书

[21] ZL 专利号 00813669.6

[45] 授权公告日 2004 年 5 月 12 日

[11] 授权公告号 CN 1149877C

[22] 申请日 2000.9.19 [21] 申请号 00813669.6

[30] 优先权

[32] 1999.10.1 [33] SE [31] 9903560-2

[86] 国际申请 PCT/SE2000/001807 2000.9.19

[87] 国际公布 WO01/026401 英 2001.4.12

[85] 进入国家阶段日期 2002.3.29

[71] 专利权人 艾利森电话股份有限公司

地址 瑞典斯德哥尔摩

[72] 发明人 J·基斯林 J·阿瓦德

B·尼尔松 B·塞克森

审查员 凌 林

[74] 专利代理机构 中国专利代理(香港)有限公司

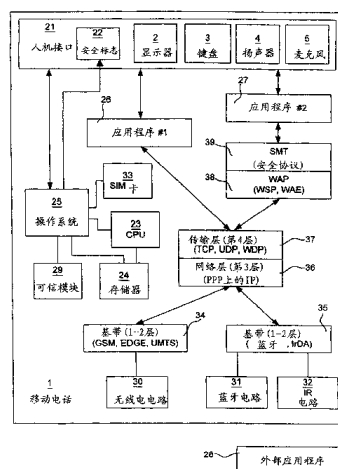
代理人 邹光新 李亚非

权利要求书 2 页 说明书 8 页 附图 4 页

[54] 发明名称 具有人机接口的一种便携式通信装置及其工作方法

[57] 摘要

一种便携式通信装置(1)有一个人机接口(2-5, 21)、一个控制器(23)、一个操作系统(25)、用于储存第一个应用程序(26, 27)的一个本地存储器(24)、只能从操作系统访问的一个安全资源(29)以及将便携式通信装置跟远程装置连接的一个无线接口(30-32)。这个人机接口让便携式通信装置的用户跟控制器和操作系统执行的第一个应用程序相互作用。这个人机接口还让用户和来自远程装置的第二个应用程序(28)相互作用。操作系统(25)并且只有操作系统能够通过人机接口(2-5, 21)提供安全标志(22)。安全标志说明安全资源(29)和当前使用人机接口的第一个和第二个应用程序(26-28)之一之间的连接是安全的。



1. 一种便携式通信装置 (1), 具有人机接口 (2-5, 21)、控制器 (23)、操作系统 (25)、用于储存第一个应用程序 (26, 27) 的本地存储器 (24)、只能由操作系统访问的安全资源 (29, 33) 和用于将
5 便携式通信装置跟远程装置 (10, 12, 15, 17, 20) 连接的无线接口 (6, 7, 30-32), 其中的人机接口用于提供便携式通信装置的用户跟被控制器和操作系统执行时的第一个应用程序之间的相互作用, 其中的人机接口还用于提供该用户和来自远程装置的第二个应用程序 (28) 之间的相互作用, 其特征在于:
- 10 操作系统 (25) 并且只有此操作系统才适用于通过人机接口 (2-5, 21) 提供一个安全标志 (22), 这个安全标志表示安全资源 (29) 与当前人机接口正使用的、第一个和第二个应用程序 (26-28) 之一的程序之间的连接是安全的。
2. 权利要求 1 的便携式通信装置, 其中的安全标志 (22) 表明当
15 前正使用的人机接口的、第一个和第二个应用程序 (26-28) 之一的程序的类型、来源, 或者当前正使用的人机接口的、第一个和第二个应用程序 (26-28) 之一的程序的认证。
3. 权利要求 1 或 2 的便携式通信装置, 其中的安全标志 (22) 被显示在便携式通信装置的显示器 (2) 上。
- 20 4. 权利要求 3 的便携式通信装置, 其中的安全标志 (22) 至少包括一个预定图标 (22a)。
5. 权利要求 3 的便携式通信装置, 其中的安全标志 (22) 包括预定文本信息 (22b)。
6. 权利要求 5 的便携式通信装置, 其中预定文本消息 (22c) 的
25 字体、大小或者颜色不同于显示器 (2) 上显示的其它文本信息。
7. 权利要求 3 的便携式通信装置, 其中的安全标志 (22d, 22e) 表明当前使用人机接口 (2-5, 21) 的、第一个和第二个应用程序 (26-28) 之一的程序是在便携式通信装置内执行的, 还是在便携式通信装置外部执行的。
- 30 8. 权利要求 3 的便携式通信装置, 其中的安全标志 (22d, 22e) 表明当前使用人机接口 (2-5, 21) 的、第一个和第二个应用程序 (26-28) 之一的程序是在制造这个便携式通信装置时最初被储存在所述

本地存储器(24)中,还是来自所述远程装置(12)。

9. 权利要求1或2中任意一个的便携式通信装置,其中的安全标志(22h)包括便携式通信装置和远程装置(10, 12, 15, 17, 20)之间连接(9, 14, 16, 19)的类型的指示。

5 10. 权利要求9的便携式通信装置,其中的连接(14, 16)是一个近距离辅助数据连接。

11. 权利要求1或2中任意一个的便携式通信装置,其中的安全标志(22)包括通过人机接口(4, 21)的音频信号。

10 12. 权利要求1或2中任意一个的便携式通信装置,其中的安全标志(22)包括通过人机接口(21)的一个可触摸信号。

13. 权利要求1或2中任意一个的便携式通信装置,其特征在于该便携式通信装置能够进行移动通信。

14. 权利要求1或2中任意一个的便携式通信装置,其中的安全标志(22)包括目前在便携式通信装置和远程装置(10, 12, 15, 17, 15 20)之间是否有一个连接的指示。

15. 权利要求1或2中任意一个的便携式通信装置,其中的安全标志(22)包括所述安全连接的物理链路质量的指示。

16. 权利要求1或2中任意一个的便携式通信装置,其中的安全标志(22)包括通过所述安全连接所进行的交易不能够用当前正使用的人机接口(2-5, 21)的、第一个和第二个应用程序(26-28)之20 一的以外的应用程序中断、操作或者解释的指示。

17. 一种操作具有能够通过人机接口执行多个应用程序(26, 27)的一个操作系统(25)这种类型的便携式通信装置(1)的人机接口(2-5, 21)的方法,其特征在于以下步骤:

25 在这个人机接口(2-5, 21)中提供一个安全性指示功能(22),提供来自所述多个应用程序(26-28)中的至少一个的用于调用安全性指示功能的操作系统,

当受到来自所述多个应用程序中的前面提到的一个的所述操作系统调用时,提供当前正使用人机接口(2-5, 21)的、所述多个应用程序(26-28)之一的安全性指示的信息,和30 在所述安全性指示功能中包括所述信息。

具有人机接口的一种便携式通信装置及其工作方法

技术领域

- 5 总的来说，本发明涉及一种便携式通信装置，用于通过它的人机接口为用户提供通信服务。具体而言，本发明涉及一种便携式通信装置，它们有控制器、操作系统、用于储存第一个应用程序的本地存储器、只能从这个操作系统访问的安全资源以及将这个便携式通信装置跟远程装置连接的无线接口。

10 背景技术

- 上述便携式通信装置的实例有移动电话、无绳电话、便携式数字助理、通信器、寻呼装置、电子付费器或者便携式导航器。在本文的以下部分中将参考 GSM、EDGE 或者 UMTS 这样的任意移动通信网络中的移动电话。但是本发明并不局限于移动电话。相反，本发明由后面的
- 15 独立权利要求加以说明。

- 传统的老式移动电话只能通过移动通信网络，在许多情况下是公共交换电话网络，在两个人之间提供语音通信。最近，移动电话有了另外的功能，比如能够在便携式通信装置和另外一个电子装置之间进行数据或者传真通信。此外，这些电话常常有简单的应用程序，比如
- 20 内置电话本、计算器、闹钟或者视频游戏。

- 再后来，移动电话采用了数不清附加的高级应用功能。这些高级应用程序包括移动电话和例如便携式计算机、打印机、无线头戴式附件等等之间进行的近距离辅助数据通信。这种近距离辅助数据通信设备的一个实例常常被叫做蓝牙设备，它工作在 2.4 GHz 的频带上，它
- 25 常常被叫做 ISM (“仪器、科学和医药”) 频带。

 高级应用程序的其它实例有无线电子付费 (“无线钱包”)、智能卡应用 (比方说 SIM 工具包应用)、到全球网络的无线访问 (比如访问因特网资源的 WAP—“无线应用协议”) 等等。

- 因此，今天的移动电话会采用许多应用程序，将来肯定也会这样，
- 30 它们共享移动电话的公共资源。共享资源包括人机接口，特别是移动电话的显示器，还包括安全或者专用资源，比方说储存在 SIM 卡 (“用户识别模块”) 或者移动电话另外一个存储器中的信息。这些应用程序

会在移动电话的不同环境中执行，例如在 WAP/Java/HTML（“超文本标示语言”）浏览器里，SIM 卡或者另一种智能卡上的处理器里执行，直接在移动电话的操作系统中执行等等。此外，一些应用程序可以在移动电话以外跟电话连接的一个外部装置中执行。此外，可以在制造好以后将应用程序下载到移动电话里。

这些应用程序中的许多可以由发生的事件激活或者启动，而不需要用户直接控制。在多数情况下，这些应用程序会通过移动电话的人机接口，特别是它的显示器，跟用户交换信息。由于显示器的大小有限，活动应用程序常常会完全控制整个显示器。激活另外一个应用程序的时候，它会接管这个显示器和人机接口的其它部分，比如移动电话的键盘。在移动电话内或者外部装置内不同环境里运行的这些应用程序之间进行突然切换，用户要注意到、理解和正确地处理非常困难。因此，用户很难发现目前突然由不同来源、不同类型或者不同环境的一个应用程序控制了这个人机接口。

此外，在低安全性环境运行的应用程序会模仿高安全性环境中运行的应用程序。例如，WAP 应用程序会假装成一个 SIM/智能卡应用程序。同样，外部应用程序会假装成移动电话内的一个应用程序。

移动电话的用户在移动电话安全资源的基础之上代替他/她进行某种安全交易的时候，以上问题是特别关心的。例如，如果这个移动电话被用作无线电子付费装置，用户通过人机接口知道他/她目前正在跟什么类型的应用程序通信，活动的应用程序是否可以相信，应用程序是否正在安全、直接地跟移动电话和人机接口的安全资源进行通信，而没有其它应用程序干预、修改或者获得通信中的任何安全数据的风险，极其重要。

可惜，在移动电话的多数应用程序环境中，保证安全性仅仅是可选的而不是必须的。例如，在 WAP 1.1 和 1.2 中，以及在 WIM（“无线识别模块”）中，WTLS（“无线传输层安全性”）这样的安全功能仅仅是一个选项。

此外，可以通过突然建立链路来激活近距离辅助数据应用程序（比如蓝牙应用程序），如果用户携带移动电话在能够进行这种通信的一个远程装置附近。

因此，对于高级应用程序，根据以上描述，移动电话用户的唯一

安全选择是核实移动电话本身，涉及到的通信标准的可选部件的采用，电话运营商提供的 SIM 卡/智能卡，以及移动电话和远程装置之间通信链路上每个节点的安全性。

发明内容

- 5 本发明的一个目的是为了给上述情形提供实质的改进，特别是让用户始终了解在移动电话的应用程序环境中目前的安全状况。

本发明中以上目的是通过提供一个安全标志来达到的，只有移动电话的操作系统能够通过电话的人机接口将这个安全标志显示给用户。最好是在电话显示器上以可视方式显示，但是也可以用能够听到或者能够触摸到的信号提供的这个安全标志，为用户提供移动电话中安全资源跟活动应用程序之间的连接的特定安全性信息，这个活动应用程序或者是在电话内部执行的，或者是在跟这个电话连接的远程装置内执行的。在这两种情况下，活动应用程序都会利用移动电话的人机接口。这个安全标志也可以说明活动应用程序的类型、来源或者证明。此外，它还可以说明这个活动应用程序的执行位置。

本发明提供如下的方法：

(一) 一种便携式通信装置，具有人机接口、控制器、操作系统、用于储存第一个应用程序的本地存储器、只能由操作系统访问的安全资源和用于将便携式通信装置跟远程装置连接的无线接口，其中的人机接口用于提供便携式通信装置的用户跟被控制器和操作系统执行时的第一个应用程序之间的相互作用，其中的人机接口还用于提供该用户和来自远程装置的第二个应用程序之间的相互作用，其特征在于

操作系统并且只有此操作系统才适用于通过人机接口提供一个安全标志，这个安全标志表示安全资源与当前正使用的人机接口的、第一个和第二个应用程序之一的程序之间的连接是安全的。

(二) 一种操作具有能够通过人机接口执行多个应用程序的一个操作系统这种类型的便携式通信装置的人机接口的方法，其特征在于以下步骤：

在这个人机接口中提供一个安全性指示功能，
提供来自所述多个应用程序中的至少一个，用于调用安全性指示功能的操作系统，

当受到来自所述多个应用程序中的前面提到的一个的所述操作系

统调用时, 提供当前使用人机接口的、所述多个应用程序中的一个的安全性指示的信息, 和

在所述安全性指示功能中包括所述信息。

以上解决方案由后面的独立权利要求给出。其它目的、特征和优点将从后面的详细说明、从属权利要求和附图中找到。

附图说明

下面将参考附图, 更加详细地描述本发明的优选实施方案和可选实施方案, 在这些附图中:

图 1 是便携式通信装置和它能够工作的应用程序环境的一个原理框图,

图 2 是图 1 所示便携式通信装置的一个框图, 和

图 3, 4a-4b、5a-5c、6 和 7 说明不同实施方案中便携式通信装置的部分人机接口。

具体实施方式

首先参考图 1, 它以移动电话 1 的形式画出了一个便携式通信装置, 还画出了它的工作环境。在正常情况下, 移动电话 1 包括一个显示器 2、一个键盘 3、一个扬声器 4 和一个麦克风 5。部件 2-5 一起形成一个人机接口, 通过它, 移动电话 1 的用户能够跟移动电话交换信息。此外, 移动电话 1 有第一个天线 6, 用于通过基站 10 跟移动通信网络 11 建立无线连接 9。移动通信网络 11 可以是一个 GSM 网络 (“全球移动通信系统”)、EDGE (“GSM 进化的增强数据率”) 或者 UMTS (“通用移动电话系统”)。移动电话 1 也可以被用于通过信关 12 在无线链路 9 上访问全球信息网络 13。全球信息网络 13 可以是因特网, 信关 12 可以是一个 WAP 服务器。

移动电话 1 还包括第二个天线 7, 它可以被用于跟一个远程装置 15 建立近距离辅助数据连接 14。如上所述, 链路 14 可以是一个蓝牙链路。远程装置 15 可以是例如打印机、传真机、无绳电话附件 (比如头戴式耳机)、计算机 (例如固定的台式计算机或者便携式膝上型计算机), 当然也可以是其它装置。

第二个天线 7 也可以用于通过信关 17 跟电子付费系统 18 建立近距离辅助数据连接 16。

除此以外, 移动电话 1 还包括一个 IR (红外) 接口 8, 利用它,

移动电话 1 可以跟远程装置 20 建立 IR 连接 19。这个远程装置 20 可以是例如（固定的、膝上型或者袖珍型）计算机、调制解调器、打印机等等。

在图 2 中更加详细地说明图 1 所示的移动电话。如上所述，电话 1 有一个人机接口 21，包括显示器 2、键盘 3、扬声器 4 和麦克风 5。中央处理单元（CPU）23 负责移动电话 1 和存储器 24 以及操作系统 25 的全面控制。中央处理单元 23 可以用任何上用微处理器或者另一种可编程电子电路实现。存储器 24 可以是随机存取存储器（RAM）、只读存储器（ROM）、可删除可编程只读存储器（EPROM、EEPROM）、快闪存储器，或者是这些存储器的任意组合。操作系统 25 最好是储存在部分存储器 24 中。

移动电话 1 还有一个 SIM 模块 33，它的形式最好是智能卡，其中储存着移动电话在移动通信网络 11 内的注册专用数据。SIM 卡 33 还可以包括一个或者多个 SIM 工具包应用程序。

移动电话 1 还有无线电电路 30，它和第一个天线 6 一起使用，建立图 1 所示的无线链路 9。类似地，移动电话 1 包括用于进行近距离辅助数据连接的电路 31，通过图 1 所示的第二个天线建立链路 14 或者 16。电路 31 可以用于例如蓝牙通信。另外，移动电话包括 IR 电路 32，用于建立到图 1 所示远程装置 20 的红外连接 19。IR 电路 32 最好用于进行 IrDA 通信。无线电电路 30、近距离辅助数据电路 31 和 IR 电路 32 都能够在市场上买到，它们不是本发明的核心部分，因此这里不再赘述。

图 2 还示出了一个可信模块（trusted module）29，它可能涉及专用密钥、秘密数据等等，跟 WIM 模块（“无线识别模块”）一起使用，用于 WAP 应用。可信模块 29 也可以跟 SWIM 模块相关，例如 SIM 卡 33 上实现的 WIM 模块。在一些实施方案中，可信模块 29 可以储存在存储器 24 里。

图 2 还说明了用于图 1 所示不同无线链路 9、14、16 的协议结构。这个协议结构基本上采用著名的七层 OSI 结构。在这个协议结构的底层有第一个和第二个基带层 34，用做到移动通信网络 11 和全球网络（因特网）13 的无线链路 9。此外，还有对应的第一个和第二个基带层 35，用于蓝牙电路 31 和 IR 电路 32。

接下来在第三层上有一个网络层，比如 PPP（“因特网协议”、“对等协议”）上的 IP。传输层 37 在第 4 层上。传输层可以是例如 TCP（“传输控制协议”）、UDP（“用户数据报协议”）或者 WDP（“无线数据报协议”）。

- 5 在第 5 层是一个 WAP 对话层 38，包括例如 WSP（“无线对话协议”）或者 WAE（“无线应用环境”）。描述 34、35、36、37 和 38 这些层的时候提到的所有协议在本领域中都是众所周知的，这里不再详细描述。

- 10 在第 6 层有一个安全协议 39，例如 SMT（“安全移动交易”）。SMT 是应用层的一个安全协议，它考虑的是跟移动个人装置进行通信的时候的局限性。目前 SMT 正在开发过程中，因此还不是一个标准。

- 15 上面描述的协议结构能够为多个应用程序提供服务，它是在移动电话 1 内部和外部的不同环境中执行的。因此，第一个应用程序 26 可以直接跟传输层 37 和人机接口 21 通信。应用程序 26 最好储存在存储器 24 中，由中央处理单元 23 在操作系统 25 里执行。另外，第二个应用程序 27 可以跟 WAP 层 38 或者安全层 39 和人机接口 21 通信。因此，应用程序 27 可以储存在存储器 24 里，由中央处理单元 23 在操作系统 25 上执行。应用程序 26 和/或 27 也可以储存在 SIM 卡 33 或者可信模块 29 里。

- 20 移动电话 1 还能够为远程装置里的外部应用程序 28 提供服务。这样一个远程装置可以是例如图 1 所示的任意装置 11、12、13、15、17、18 或者 20。这样一个外部应用程序 28 通过人以一个无线链路 9、14、16 或者 19（也就是无线电近距离辅助数据或者红外链路）跟移动电话 1 通信。用户通过移动电话 1 的人机接口 21 跟外部应用程序 28 相互作用。

- 25 为了上面提到的本发明的目的，为移动电话提供了一个安全标志 22，它是人机接口 1 的一部分，只能从操作系统 25 对它进行控制。此外，应用程序 26、27、28 只能够通过操作系统 25 的特定操作系统调用来影响安全标志 22。这样，没有任何应用程序能够在没有操作系统 25 的协作和同意下修改安全标志 22。根据本发明的不同实施方案，安全标志 22 包括一个或者一个以上的特殊图标（图 3 中的 22a），它最好驻留在显示器 2 的某个位置上，只能通过操作系统调用，由操作系统 25 更新。另外，这个安全标志可以是一个特殊的字母数字字符，或
- 30

者是一个特殊的文字信息(图 4a 中的 22b), 它的字体(图 4b 中的 22c) 大小或者颜色不同于显示器 2 上面的正常文本信息(图 3 中的 42 和 43)。图 3 中的图标 40 和 41 分别是信号强度和电池容量的一般标志。

5 作为以上类型安全标志的一个选择, 安全标志 22 也可以是可以通
过移动电话 1 的扬声器 4 听到的音频信号。作为另一个选择, 安全标
志可以是移动电话 1 中其它装置产生的能够触摸到的信号(最好是一个
振动信号)。

安全标志 22 的目的是通过人机接口 21 告诉用户当前跟用户通信
的活动应用程序的安全级别。由于只能由操作系统 25 控制安全标志
10 22, 因此用户可以相信安全标志提供的信息。根据一个实施方案, 安
全标志可以说明用户目前通过人机接口 21 进行通信的活动应用程序的
类型、安全级别或者来源。例如, 如图 5a 所示, 安全标志 22d 可以说
明活动应用程序是一个本地程序(储存在移动电话 1 并且由移动电话 1
执行)。对应地, 在电话 1 外面的一个远程装置里储存和/或执行的外
15 部应用程序也可以通过安全标志 22e 说明(图 5b)。如图 5c 所示, 安
全标志 22f 可以说明活动程序更加具体的类型, 例如它是一个 SIM 工
具包应用程序。安全标志还可以说明活动应用程序在 WAP/Java/HTML
浏览器中运行。

或者安全标志 22g 可以说明活动应用程序已经通过某种方式被证
20 实(图 6)。安全标志还可以说明从以前的活动应用程序向当前活动应
用程序的切换。

根据一些实施方案, 安全标志可以说明移动电话 1 中是否在制造
过程中提供了活动应用程序, 或者这个活动应用程序是早些时候下载
到电话 1 中的。

25 如果当前的活动应用程序是一个外部应用程序, 安全标志 22 就可
以说明移动电话 1 和外部应用程序所在远程装置之间链路的安全级
别。安全级别可以随后用图 3 中的图标 22a 以图形方式说明。图标 22a
的三个钥匙图案代表高级别的安全性, 两个钥匙代表中等程度的安全
性, 一个钥匙代表安全级别较低, 没有钥匙表示没有安全性。

30 安全标志(图 7 中的 22h)也可以说明移动电话和远程装置之间链
路的类型, 比方说蓝牙链路(14、16)、红外链路(19)或者无线电链
路(9)。

此外，安全标志 22 还可以说明活动程序当前进行的交易是原子的，也就是说这一交易不能被打断、操纵，也不能被这个活动应用程序以外的任何其它应用程序解释。安全标志 22 还可以说明这种安全交易的重要参数，比方说所用加密方法的密钥长度等等。

- 5 此外，安全标志 22 还可以说明目前是否建立了无线链路 9、14、16 或者 19 中的任何链路，它的安全状态，或者建立起来的这样一条链路的物理质量（信号强度等等）。

- 10 综上所述，本发明通过便携式通信装置的人机接口提供一种安全标志，其中的安全标志代表便携式通信装置的安全源跟当前正在使用这个人机接口的活动应用程序之间连接的安全性。安全资源这个术语指的是移动电话 1 的某个部分（例如它的人机接口 21），储存在移动电话中的专用密钥或者其它安全数据，例如储存在可信模块 29、存储器 24 或者 SIM 卡 33 中。

- 15 上面参考附图描述了本发明。但是除了上面描述的实施方案以外，本发明的范围内还有其它实施方案，这些其它实施方案由后面的独立权利要求定义。

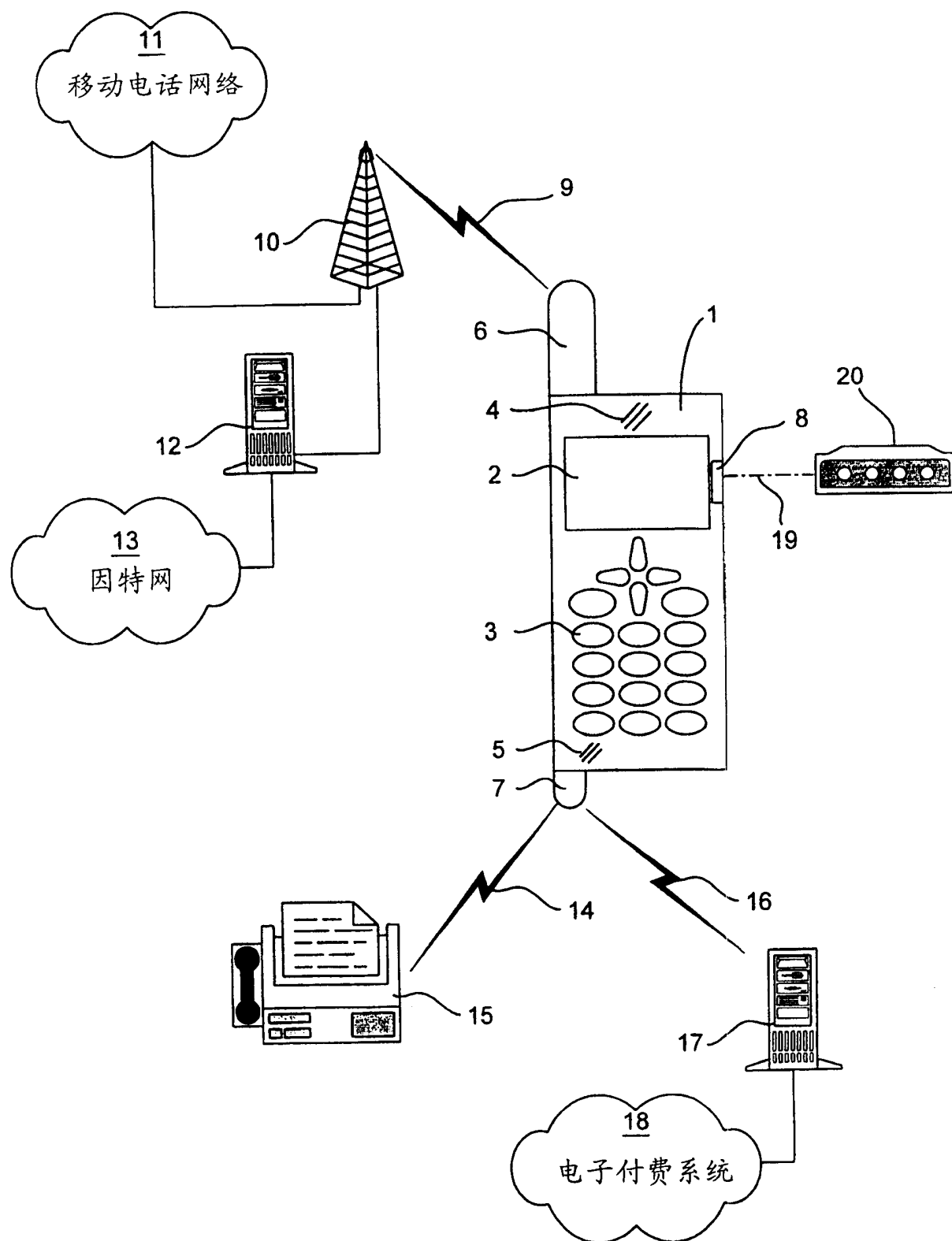


图 1

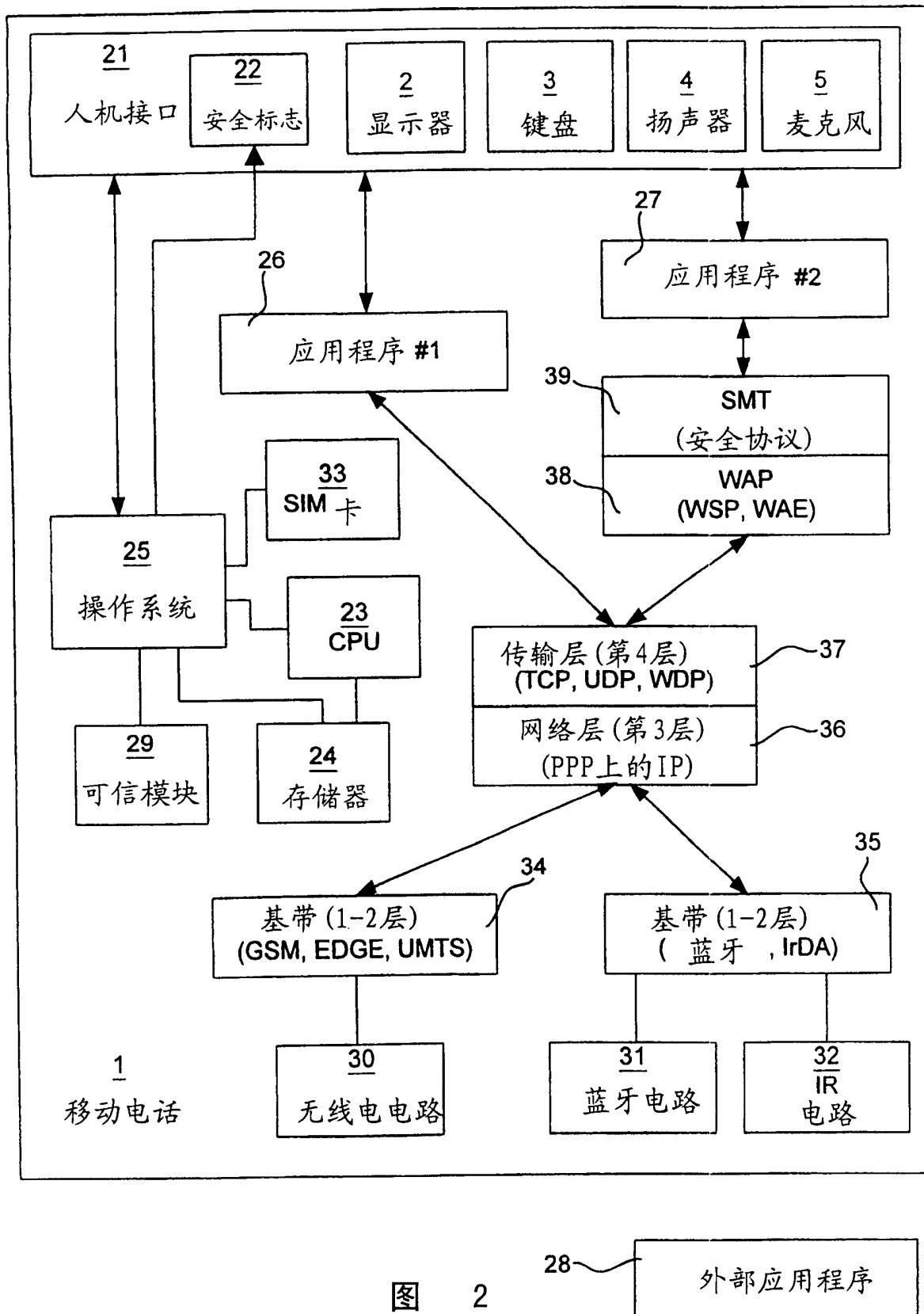


图 2

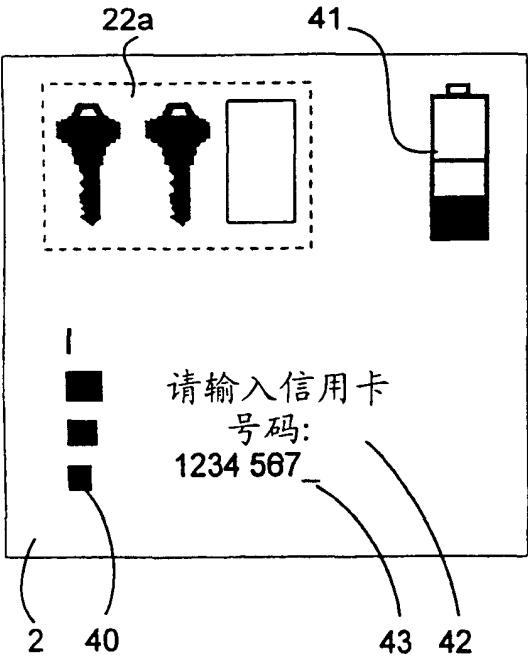


图 3

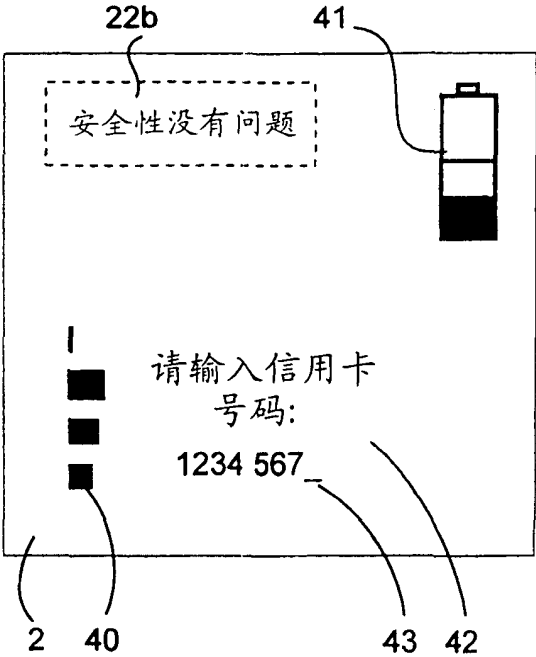


图 4a

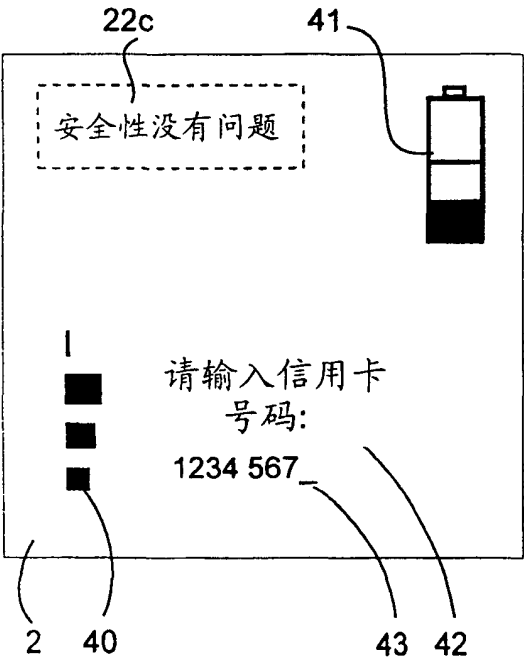


图 4b

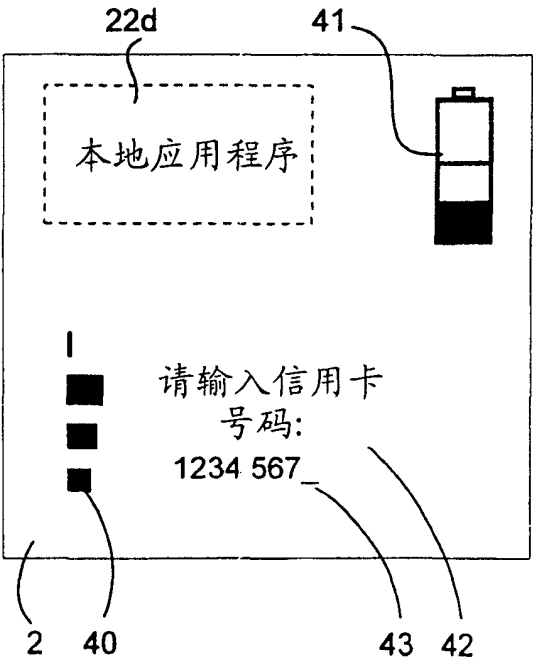


图 5a

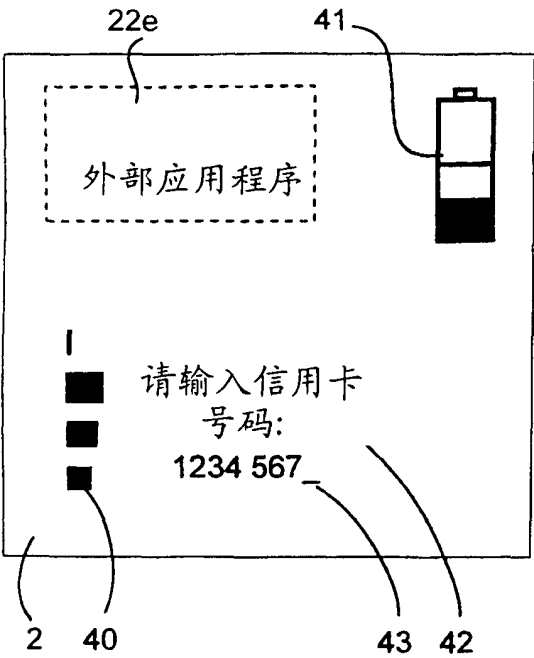


图 5b

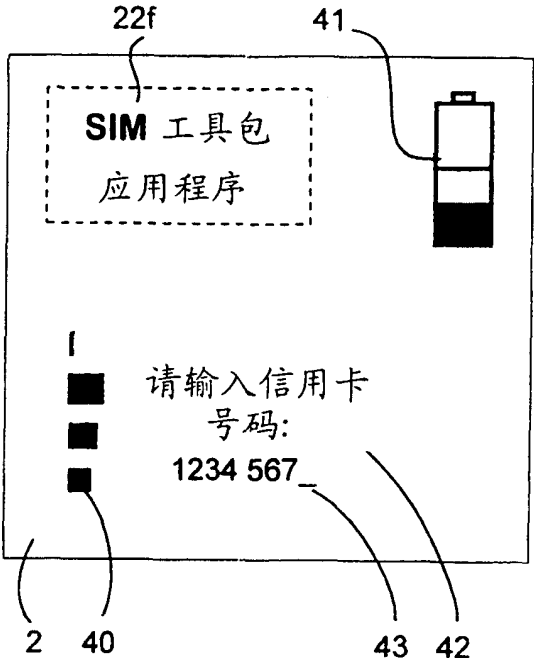


图 5c

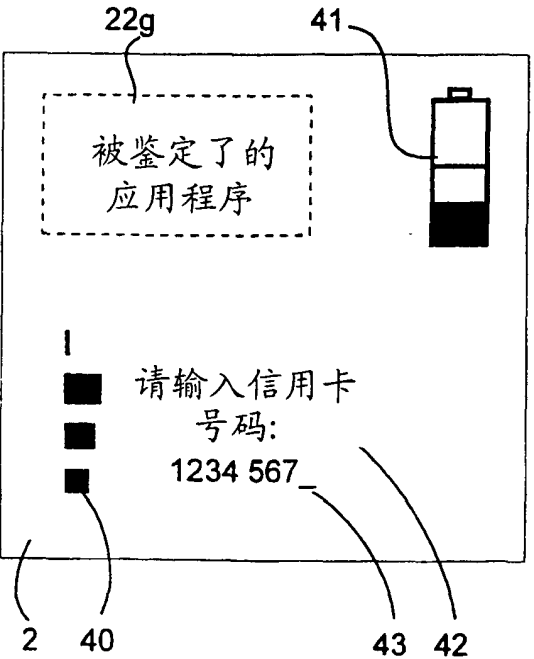


图 6

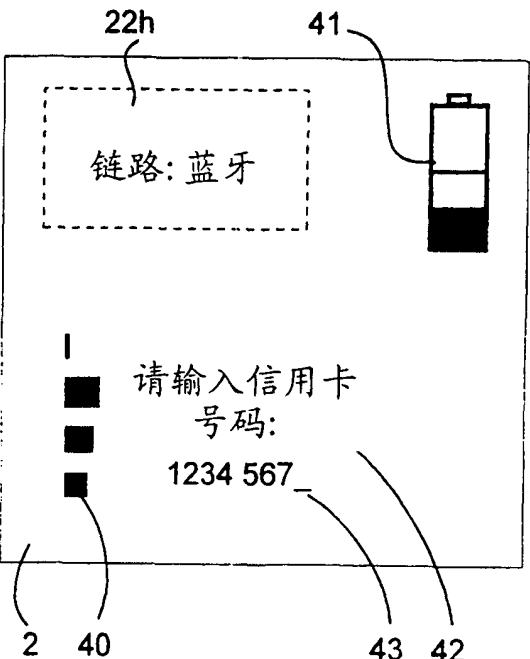


图 7